UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/916,785
Filing Date: July 27, 2001
Appellant(s): SEROUSSI ET AL.

Robert W. Bergstrom
Reg. No. 39,906
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/30/2007 appealing from the Office action mailed 10/3/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect.

The appellant filed an Amendment After Final on 12/15/05. The amendment after final rejection filed on 12/15/05 has not been entered.

The appellant filed an Amendment After Final on 7/31/06. The amendment after final rejection filed on 7/31/06 has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,430,170 Saints et al. 8-2002

Eastlake et al., "Randomness Recommendations for Security", RFC 1750, 12/1994, pg. 1 - 30.

Microsoft Press Computer Dictionary 3rd ed., 1997, Microsoft Press, pages 107, 396, 426, 510.

Strobel, Nick, "Electromagnetic Radiation", 5/17/2001, www.astronomynotes.com/light/s1.htm, accessed 9/11/07 via web.archive.org., pages 1-28.

Newton, Harry, Newton's Telecom Dictionary 12th ed., 1997, Flatiron Publishing, page 156.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 10 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake et al. (Eastlake), "Randomness Recommendations for Security", RFC 1750 in view of Saints et al. (Saints), "Method and Apparatus for Generating Random Numbers From a Communication Signal", U.S. Patent 6,430,170.

Regarding claims 10 – 13, Eastlake discloses techniques for generating random numbers, essentially comprising the method gathering low quality random data from one or more sources, processing such low quality random data to produce higher quality random data, and finally processing such higher quality random data to generate usable random values (Eastlake, page 27, section 9 -"Conclusion").

Thus, specifically regarding claim 10, Eastlake discloses:

an environmental sensor that generates digitally encoded sensor values (Eastlake, page 10, section 5; page 8, section 4.2; page 14, section 5.3.1-2). Herein, Eastlake teaches the detection of a multitude of environmental parameters (i.e. mouse movements, network packet arrival times, user keystrokes, thermal noise, radioactive

decay, sound, disk drive fluctuations, etc.) so as to provide a random bit stream [bit string - digitally encoded values] (Eastlake, page 1, abstract; page 27, section 9);

a compressor that receives the digitally encoded sensor values generated by the environmental sensor and compresses the received digitally encoded sensor values to generate a compressed data stream (Eastlake, page 14, section 5.3.1; see also pages 10 - 14, sections. 5.2 – 5.3.1). Eastlake discloses, for example in section 5.3.1, a compressor within a Unix system that receives the output of a sensor (the dev/audio device) so as to use reversible compression to de-skew the collected bit stream as taught in section 5.3.4. Furthermore, in the above cited portions, Eastlake enables the use of compressing means ("compressors") through the teachings that gathered bit streams may be compressed or reduced in size via a multitude of techniques such as – mapping longer strings of bits to shorter strings of bits, the discarding of non-overlapping bit pairs within the streams, the removal of strong correlations within bit streams, and by the use of reversible compression techniques to remove certain bits found within the bit streams. In each of these techniques, Eastlake discloses compressing or reducing the size of a set of gathered data ("compress" - if necessary, the applicant may refer to evidence of the definition of compress – "To reduce the size of a set of data…", Microsoft Press Computer Dictionary 3rd ed., pg. 107).

a random number generator that receives data from the compressed data stream and outputs random numbers (Eastlake, page 27, section 9, par. 3; page 20, par. 1 – 4). Eastlake discloses a random number generator that takes the gathered seed data ("seed" – an input value that is processed by the random number generator to output

random numbers - if necessary, the applicant may again refer to the Microsoft Press Computer Dictionary 3rd ed., pg. 426) and outputs random numbers.

Eastlake discloses recommended random number generation techniques via the collection of "quality" data. Eastlake teaches that after a sufficient amount of random seed data is collected, then the random number generator can output a "cryptographically strong" random number (Eastlake, pg. 27, section 9, par. 3). However, Eastlake does not appear to explicitly state the elements necessary to determine when a sufficient amount of random data has been gathered by the system. Namely, Eastlake does not appear to explicitly disclose *a monitor that receives the compressed data stream and monitors the compressed data stream to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number; and a blocking switch controlled by the monitor to block output of a next random number by the random number generator when sufficient data to generate the next random number has not been received in the compressed data stream to generate a next random number.*

Like Eastlake, Saints also discloses the generation of random numbers via the gathering and processing of random input bit streams (Saints, Abstract). The method of Saints utilizes a random number generator unit (fig. 4:312) that receives random bits resulting from the measurement of thermal noise (Saints, 5:26-31; 7:1-7) by environmental sensors (Saints, 5:66-6:14; fig. 2). The gathered random data is processed to ensure that the random data bits are of an acceptable quality (Saints, 9:1-7). The gathered random data bits are stored in a memory ("pool buffer" – Saints, fig.

4:406), wherein after a sufficient amount is gathered, the data is transmitted to and processed by a function that extracts randomness (for example, a hashing function) and finally a random number is output from the random number generator unit (Saints, 7:36-49). After a random number is output, the process can be repeated to form a new random number (Saints, 10:3,4). In addition to the methods shown by Eastlake, Saints discloses, in particular, a way to determine that a sufficient amount of random data has been gathered by the system so as to output the random number. Namely, Saints teaches "*a monitor*" – wherein during the process of adding random data bits to the pool buffer – a system element employs a counter to advance through the pool buffer, wherein until the counter reaches the end of the pool buffer, the pool is not ready for use [i.e. to output a random number] (Saints, 9:8, 9, 15-18, 30-38). Furthermore, Saints discloses "*a blocking switch*" – wherein after a random number has been extracted from the pool, and the used data bits within the pool have been discarded (Saints, 9:35-38) – a system means is employed to release a random number from the buffer pool as soon as the buffer pool becomes filled, wherein, a random number is not released from the pool until the system determines that the counter has reached the end of the pool (Saints, 10: 3,4; 9:57,58, 8, 9, 32–34).

It would have been obvious to one of ordinary skill in the art to combine the practical teachings of Saints (for providing "a monitor" and "blocking switch" system means to monitor the collection of random data and prevent the output of a random number until sufficient random data has been collected) with the recommended methods of Eastlake. This would have been obvious because one of ordinary skill in the

art would have been motivated by the need to determine when a sufficient amount of random data has been gathered and subsequently enable the output of "quality" or cryptographically strong random values as taught to be necessary by Eastlake (see Eastlake, page 27, section 9, par. 3).

Regarding claim 11, the combination of Eastlake and Saints enables:

one or more additional environmental sensors (Eastlake, page 10, section 5; page 8, section 4.2; page 14, sections 5.3.1-2; page 27, section 9, par. 2). Herein, and as show above regarding claim 1, the combination enables a plurality of usable environmental sensors and using them in combination.

an additional compressor for each of the one or more additional environmental sensors (Eastlake, page 27, section 9, par 2; page 14, section 5.3.1, par. 3; page 13, section 5.2.4, par. 2). As clearly shown above, the combination enables the utilizing and processing of multiple sources to generate "random" bit streams. One such source could be an audio bit stream detected by a microphone. The output of the sensor ("microphone") is concatenated with a compressor employing a reversible compression technique. Of course, Eastlake shows that such a compressed data stream will not be of very high "random" quality, and thus should be viewed as a rough technique in light of the additional techniques available for random number generation utilizing data gathered by environmental sensors (for example, see Eastlake, pages 13 –14, sections 5.2.4 – 5.3.1). Furthermore, another such usable environmental source, as enabled by the combination, is the detection of disk drive operation and the necessary processing

of this "highly correlated" data using FFT, another function that effectively reduces the size or compresses the measured bit stream so as to generate a "random" bit stream (for example, see Eastlake, page 14, section 5.3.2 and page 13, section 5.2.3).

and a merging component that merges the compressed data streams output by the compressors to produce a merged, compressed data stream that is output to the monitor and random number generator (Eastlake, page 27, section 9, page 19, section 6.2, par. 3; page 14-15, section 6). Herein the combination enables for the collected "random" bit streams to be used to produce usable random numbers via the utilization of a *"merging component"* – namely a means for the collected bit streams (for example, such as by the audio data and/or the disk drive methods discussed above) to be combined and further processed by a mixing function.

Regarding claim 12, the combination of Eastlake and Saints enables:

wherein the random number generator applies a hash function to the received data to produce a random number for output by the random number generation device (Eastlake, page 18, section 6.1.5, par. 4; page 19, section 6.3.1; Saints, fig. 4:408).

Regarding claim 13, the combination of Eastlake and Saints enables:

wherein each environmental sensor monitors an environmental parameter, the environmental parameter selected from among environmental parameters including: temperature; sound; motion; light intensity; and ambient electromagnetic radiation (Eastlake, page 10, section 5; page 8, section 4.2; page 14, section 5.3.1-2). As

previously discussed regarding claim 1, Eastlake clearly shows that the environmental sensors monitor an environmental parameter. It is noted by the examiner that the claim recitations do not require that a plurality of different environmental parameters be monitored by the sensors nor the inclusion of each of the environmental parameters recited by the applicant as usable for monitoring. Nevertheless, the examiner points out that Eastlake teaches that usable environmental parameters may comprise "motion" such as a user's mouse movements or a user's key strokes, the monitoring of "sound" such as audio from a microphone, or the monitoring of thermal noise, i.e. a parameter of "ambient electromagnetic radiation" and "temperature" (it is noted that the applicant can refer to evidence such as "Electromagnetic Radiation", pages 8, 11 – 14 by Nick Strobel).

(10) Response to Argument

Before addressing the appellant's arguments, the examiner notes that it may be helpful to clarify some issues regarding the terminology used within the appellant's arguments and claims.

(1) "stream"

The appellant's claims and arguments comprise repeated use of the term "stream". Of course, when considering the appellant's arguments and claims, it would also be helpful to consider exactly what is meant by the appellant (or at least what is in harmony with the appellant's original disclosure) regarding this term "stream". Quite

simply, according to the appellant, a "stream" is or can be interpreted to be a string or sequence of bits (for example, see appellant's specification, page 3, lines 25,26; page 4, line 30). Herein, the appellant describes a sequence of a distinct number (K) of bits as a stream [**K bit**-streams]. Also, the appellant refers to a "word", a distinct and limited number of bits, as a stream ("word", see Microsoft Press Computer Dictionary 3rd ed., pg. 510).

The examiner feels that this clarification is necessary as the appellant's arguments, as addressed below, appear to assert that claim recitations of a "stream" define over the prior art.

(2) "compression"

The appellant's arguments largely comprise assertions such as that the prior art does not disclose "compression", a means for compressing ("a compressor"), or "a compressed" stream of data. Thus, the examiner notes that it would be helpful to consider the definition of "compression" as would have been understood by one of ordinary skill in the art.

Regarding the compression of data, the Newton's Telecom Dictionary, 12th ed. states: "Data Compression…(1). The process of reducing (a) bandwidth …for the generation, transmission, and storage of data by employing techniques designed to remove data redundancy."

"Compress", as revealed by The Microsoft Press Computer Dictionary 3rd ed., page 107, means "To reduce the size of a set of data…". The dictionary further

discusses that "Data can be compressed by removing repeated patterns of bits and replacing them with some form of summary that takes up less space..".

"Compressor", as revealed by The Microsoft Press Computer Dictionary 3rd ed., page 107, is a "device that limits some aspect of a transmitted signal, such as volume…"

"Data Compression", as revealed by The Microsoft Press Computer Dictionary 3rd ed., page 130, is a "means of reducing the amount of space or bandwidth needed to store or transmit a block of data…",

Appellant's arguments filed 4/30/2007 have been fully considered but they are not persuasive.

The appellant argues or asserts primarily that:

(i) *Eastlake does not teach such a compressor. Instead, Eastlake is a general, review article that mentions a variety of different security related techniques. Eastlake does mention using thermal noise as a physical source of unpredictable numbers, in Section 5, but does not teach, mention, or suggest using the physical source as a continuous source of random bits for generating a compressed data stream.* (Arguments, page 5, par. 1)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies

(i.e., *using the* ***physical source as a continuous source*** *of random bits for generating a compressed data stream*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Additionally, in response to applicant's argument that "*Eastlake does not teach, mention, or suggest using the physical source…* ***for generating a compressed data stream"***, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Finally, it is respectfully noted that the prior art clearly does disclose a compressor (Eastlake, page 14, section 5.3.1, see also rejection of claim 10) that receives digital data from environmental sensors and compresses the received digital data (*digitally encoded sensor values*) so as to generate an output of compressed digital data (*compressed data stream*).

(ii) *Eastlake does not disclose a compressor that receives digitally encoded sensor values and generates from the digitally encoded sensor values a compressed data stream. In Section 5.2.4, Eastlake mentions using a reversible compression technique to deskew a skewed bit stream. However, Eastlake does not, in Section 5.2.4, disclose*

or suggest the source of the bit stream, and does not suggest a compressed-data-stream output. (Arguments, page 5, par. 1)

In response, the examiner respectfully notes that the appellant's assertions (i.e. that prior art fails to disclose a compressor and an output of the compressor) are substantially similar to the above argument (ii) of the appellant. The examiner finds the appellant's argument unpersuasive for the same reasons stated above. Furthermore, the examiner respectfully directs one's attention to the prior art, wherein the prior art teaches a compressor (Eastlake, page 14, section 5.3.1, par. 3), a digital input stream to a compressor (Eastlake, page 13, section 5.2.4, par. 1, 2; page 14, section 5.3.1, par. 1), a digital output stream of a compressor (Eastlake, page 13, section 5.2.4, par. 1, 2; page 14, section 5.3.1, par. 3), and that digital output of a compressor comprises compressed output (Eastlake, page 13, section 5.2.4, par. 1, 2) .

It is also noted that the appellant admittedly recognizes an input to a compression means – "*Eastlake mentions using a reversible compression technique to deskew a skewed bit stream"*. However, the appellant appears to proceed in asserting that the prior art makes no disclosure or suggestion that the input ("*a skewed bit stream"*) has a source ("*However, Eastlake does not…disclose or suggest the source of the bit stream"*). In response to this, the examiner points out that the prior art clearly discloses that the skewed input streams have sources (for example, see Eastlake, page 14, section 5.3.1 – herein a source [i.e. a "huge amount" of digitized data produce via the sensing of thermal noise]).

(iii) *Moreover, in Section 5.2.1, Eastlake computes a number of bits that need to be sampled in order to produce a deskewed result, indicating again that Eastlake envisions obtaining sufficient bits from a physical source to generate a seed, rather than a compressed stream of data.* (Arguments, page 5, par. 1)

In response, the examiner respectfully notes that the appellant appears unpersuasive. Namely, section 5.2.1 of Eastlake clearly discusses one method to produce a randomly distributed output from a sampled input (Eastlake, page 11, par. 1; page 12, par. 2,3). Eastlake calls such method "Using Stream Parity to De-Skew". Of course, however, the method cannot just be used blindly without attention to the details necessary for achieving a randomly distributed output. Thus, Eastlake discloses these necessary details which would include an estimate of how many input bits within a bit stream will result in an output bit steam that could be considered to have a random distribution. Once a person realizes the statistical nature of the process, a person may then effectively utilize stream parity to de-skew an input bit stream – which according to Eastlake, comprises taking a larger input stream and reducing it in size to a smaller output stream, "compression".

Thus, the examiner points out that a careful consideration of Eastlake reveals no basis for the appellant's conclusion *that Eastlake envisions obtaining sufficient bits from a physical source to generate a seed, rather than a compressed stream of data.*

(iv) *Finally, Eastlake makes no mention of a random number generator implementation that includes a compressor component that receives digitally encoded sensor values and that generates a compressed data stream.* (Arguments, page 5, par. 1)

The examiner respectfully notes that the appellant's argument is essentially the same as argument (ii). Thus, examiner notes that this assertion is unpersuasive, at least, for the same reasons as discussed above.

(v) *Eastlake does indeed disclose, in Section 6, obtaining random input from a large number of uncorrelated sources and mixing them with a strong mixing function. However, Eastlake does not disclose that the large number of uncorrelated sources are compressed data streams.* (Arguments, page 5, par. 2 – page 6)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *the large number of uncorrelated sources are compressed data streams*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Furthermore, it is respectfully noted that neither the examiner nor the prior art has asserted or suggested that "sources are compressed data streams".

(vi) *Instead, as explicitly disclosed by Eastlake in Section 6.3, Eastlake envisions using random bits, mixed by strong mixing functions, to generate a strong random seed that is the initial input into a cryptographic algorithm that then produces a series of random numbers. Thus, Applicants' representative respectfully disagrees that Eastlake discloses "a compressor that receives the digitally encoded sensor values generated by the environmental sensor and compresses the received digitally encoded sensor values to generate a compressed data stream."* (Arguments, page 6, lines 2 – 8)

In response, the examiner respectfully notes that it again appears that appellant is making an unsupported jump to an erroneous conclusion. Namely, section 6.3 of Eastlake is clearly disclosing the operation of a random number generator that utilizes gathered seed material. Appellant is respectfully encouraged to examiner section 6.3 within context. For example, one may simply refer to page 9, section 9 of Eastlake to see that Eastlake's discussion of random number generation includes the process of gathering a sufficient amount of random bits "seed material" which is subsequently processed by the random number generator to output a random number (refer back to section 6.3). As was already noted in abundance, Eastlake clearly discusses the sources of his gathered seed material (i.e. digitized inputs sampled from analog sources such as thermal noise). The examiner notes that this exact same process as disclosed by Eastlake for gathering bit streams from environmental sources, compressing the received data to improve the random quality of the collected data (Eastlake, sections 5

– 5.3.2), subsequently processing them by a generator (Eastlake, sections 9 and 6.3), and then outputting random numbers (Eastlake, section 6.3) is mirrored by the appellant (Appellant's specification, Abstract).

(vii) *Thus, the pool is not a compressed data steam generated from digitally encoded sensor values. Instead, the pool contains random numbers, generated by a hash function, from energy samples.* (Arguments, page 6, par. 2)

In response, the examiner respectfully points out that the appellant's argument against the reference of Saints appears to be based upon an assertion against the notion of the pool buffer of Saints being a compressed data stream.

However, it is noted that neither the examiner nor the prior art references has ever stated or implied that the pool buffer of Saints was a compressed data stream. Clearly and explicitly stated by Saints, the pool is a buffer that stores the collected bits, such that the gathered bits may be processed and a random number be output from the generator (See Saints, fig. 4 elements 312, 406, and "Random Number"; see also Saints 2:43-56; 8:51 – 9:58).

Furthermore, as can be best understood by the examiner, the examiner notes that it appears that the appellant may be implying that Saints does not disclose storing compressed data bits within the pool buffer.

If this is the position take by the appellant, then the examiner must point out that Saints has not been relied upon to demonstrate the compression of sampled

environmental data. Eastlake has already pointed out that sampled data should be compressed before being suitable to serve as seed material within a random number generator. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(viii) *The Examiner apparently relies on a single sentence from Saints, on lines 57-58 of column 9, for disclosing the monitor element of claim 10. That line states:*

> *In a preferred embodiment, as soon as the pool is filled, a random number will be extracted from the pool.*

As explicitly stated by Saints, the pool generally contains multiple random numbers, and not a compressed data stream. This single sentence of Saints basically states that a buffer, or pool, of random numbers is first filled, and after the pool is filled, extraction of random numbers from the pool begins. There is no suggestion that a compressed data stream is continuously monitored by a monitor component to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number.

Contrary to the appellant's assertion – "*This single sentence of Saints basically states that a buffer, or pool, of random numbers is first filled, and after the pool is filled, extraction of random numbers from the pool begins.*" – it is respectfully noted that this single sentence is basic and clear enough to be interpreted exactly the way it was written – namely "as soon as the pool is filled, a random number will be extracted". Simply put, should one read in context, one will note that the "filling" of the pool is a

reference to the placing of collected bits into the buffer [Saints, 2: 43-56; 9:15-40], and that the "extracting" of a random number is a reference to the process of hashing a block of random bits from the pool and outputting the result [Saints, 9:41-45].

Furthermore, it is noted that *"continuously monitored"* is not a claim recitation. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *continuously monitored*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(ix) *…it is clear that random number generation is not blocked until sufficient random bits to generate a next random number have been accumulated* (Arguments, page 7, par. 2)

In response, the examiner respectfully notes that the claim language recites "to block output of a next random number". In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *random number generation is not blocked until sufficient random bits to generate a next random number have been accumulated*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(x) *The cited passage of Saints, in combination with the preceding and following textual context from which it was taken by the Examiner, does not suggest a continuous monitoring of an input stream to determine whether or not sufficient data has been obtained to generate a next random number… Quite often, in automated systems, a first portion of a program execute, to initialize data structures and variables, before a steady-state, continuously executing portion of the program begins to execute. Such initialization code is not referred to as, nor considered as, a monitor. Initialization code generally executes once as the program begins execution, to prime execution of the bulk of the program, and is generally not subsequently executed during the remaining execution of the program. The cited passage of Saints describes such an initialization routine, and therefore does not describe, and is not relevant to, the claimed monitor that that receives the compressed data stream and monitors the compressed data stream to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number.* (Arguments, page 7, par. 1)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *a continuous monitoring of an input stream*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Furthermore, the examiner respectfully notes that the prior art makes no mention of the appellant's characterized "*initialization code*". Also, the examiner has never asserted the "initialization code", as introduced by the appellant, to be "a monitor".

(xi) *There is no mention in lines 30-59 of column 9 of Saints of a blocking switch, or any other kind of switch.* (Arguments, page 8, par. 1)

In response, the examiner points out that the appellant's claims recite a *"blocking switch"*, such recitation qualified only by the functionality provided by the "blocking switch". For example - *to prevent the random number generator from outputting a random number* (Appellant's specification, page 6, line 13), *the blocking function* (page 6, line 26), and so that *the device can be "unblocked"* (quotations by the applicant, page 6, line 31, 32).

The examiner respectfully maintains that the prior art discloses a system means for preventing the output of a random number from the generator until sufficient data has been received, and therefore a "blocking switch", (see the rejection of claim 10, above).

(xii) *There is no mention in the cited lines of Saints that a monitor enables and disables random-number generation, using a blocking switch, as a result of monitoring*

an input compressed data stream. Instead, in the cited lines, as discussed above, Saints describes … (Arguments, page 8, par. 1).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted, as was noted regarding appellant's argument (x), that the features upon which applicant relies (i.e., *disables random-number generation, using a blocking switch*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(xiii) *As discussed above, Saints neither discloses, teaches, mentions, nor suggests a monitor to monitor the collection of random data and neither discloses, teaches, mentions, nor suggests a blocking switch to prevent random number generation until sufficient random data has been collected. Instead, the single sentence from column 9 to which the Examiner appears to attribute these components of the claimed random number generator simply states that a random number can be extracted from a pool of generated random numbers once the pool of generated random numbers is filled.* (Arguments, page 8, par. 1)

In response, the examiner notes that this argument (i.e. that prior art does not teach a blocking switch that prevents random number generation, that the examiner

relies only on a single sentence) is substantially similar to preceding arguments. Therefore, the examiner finds it to be unpersuasive for the same reasons.

(xiv) *The Examiner repeatedly refers to the term "quality random number," although Applicants' representative cannot find this term in either of the cited references or the current application. The justification for combination is thus, in part, based on a term that is not defined by the Examiner, and that does not appear to occur in either the cited references of the current application.* (Arguments, page 8, par. 1 – page 9, line 1)

In response, it is noted that the examiner had *twice* used the term "quality random number". This, of course, is entirely understandable to one of ordinary skill in the art as a prime objective in random number generation is to produce values that are of a sufficient quality - "cryptographically strong" - values that could or would be considered random. In fact, a cursory review of Eastlake shows, at least 8 times, the usage of the term "quality" in relation to random data. The appellant also appears to recognize the relationship between randomness and quality, as the appellant admits to the desire to "prove an *improved* random sequence generator" (Appellants specification, page 2, par. 1).

Thus, the examiner respectfully asserts that provisions for ensuring that "quality"/"cryptographically strong"/"acceptable" random numbers are generated is entirely a justified basis for the prior art combination.

(xv) *Neither Eastlake nor Saints teaches, mentions, or suggests any kind of blocking of random number generation based on waiting a sufficient amount of time for gathering sufficient random input data… The cited portion of Saints does not disclose or suggest a monitor and blocking switch that together wait a sufficient amount of time to generate a random number from the compressed output of an environmental sensor.* (Arguments, page 9, par. 1)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *blocking of random number generation based on waiting a sufficient amount of time for gathering sufficient random input data; a monitor and blocking switch that together wait a sufficient amount of time to generate a random number from the compressed output of an environmental sensor*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(xvi) *Regarding the rejection of claim 11, the Examiner states … Applicants' representative believes that the Examiner is referring to the following paragraph from Section 6 of Eastlake …*

This statement has nothing at all to do with environmental sensors or mixing together the random input of environmental sensors. Instead, as the title for the section,

"Recommended Non-Hardware Strategy," suggests, this section of Eastlake refers to using strong mixing functions to mix pseudorandom numbers from various sources together to produce a more random output. Eastlake is referring to non-hardware pseudorandom number sources, rather than to sensors or other such physical devices. (Arguments, page 9, par. 2, 3)

In response, the examiner respectfully points out that references are to be considered in their entirety, and that the examiner cites numerous portions, of Eastlake, wherein Eastlake abundantly shows the detection of signals from a multitude of sources within the environment and teaches the idea of detecting these multiple sources in combination. It can be clearly seen that Eastlake discloses detecting input from a multitude of environmental sources (i.e. humans, software, hardware, physical phenomena). In order to detect input from a source, a means for input detection ("a sensor") is required.

Furthermore, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *sensors or other such physical devices*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(xvii) *As discussed above, Eastlake does not even disclose a single compressor component for a random-number-generator device.* (Arguments, page 10, lines 2, 3)

In response, the examiner notes that this argument is substantially similar to arguments previously address, and is found to be unpersuasive for the same reasons.

(xiii) *Regarding the rejection of claim 13, the Examiner cites several sections of Eastlake that refer to several sources of random bits…From these modest suggests that include essentially only one type of environmental sensor, namely a thermal noise sensor … Applicants' representative respectfully observes that obviousness-type rejects require at least a clear suggestion, and that a thermal sensor does not suggest sound, motion, light-intensity, and electromagnetic radiation sensors.* (Arguments, page 10, par. 1)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *sound, motion, light-intensity, and electromagnetic radiation sensors*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Furthermore, as previously discussed, Eastlake disclosing sensing input from a plurality of sources within the environment (i.e. humans, software events, hardware, physical phenomena) and therefore enables a means to sense ("sensors").

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Jeffery Williams/
Examiner, Art Unit 2437

Conferees:

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

/Matthew B Smithers/
Primary Examiner, Art Unit 2437